



ITIL GUIDE

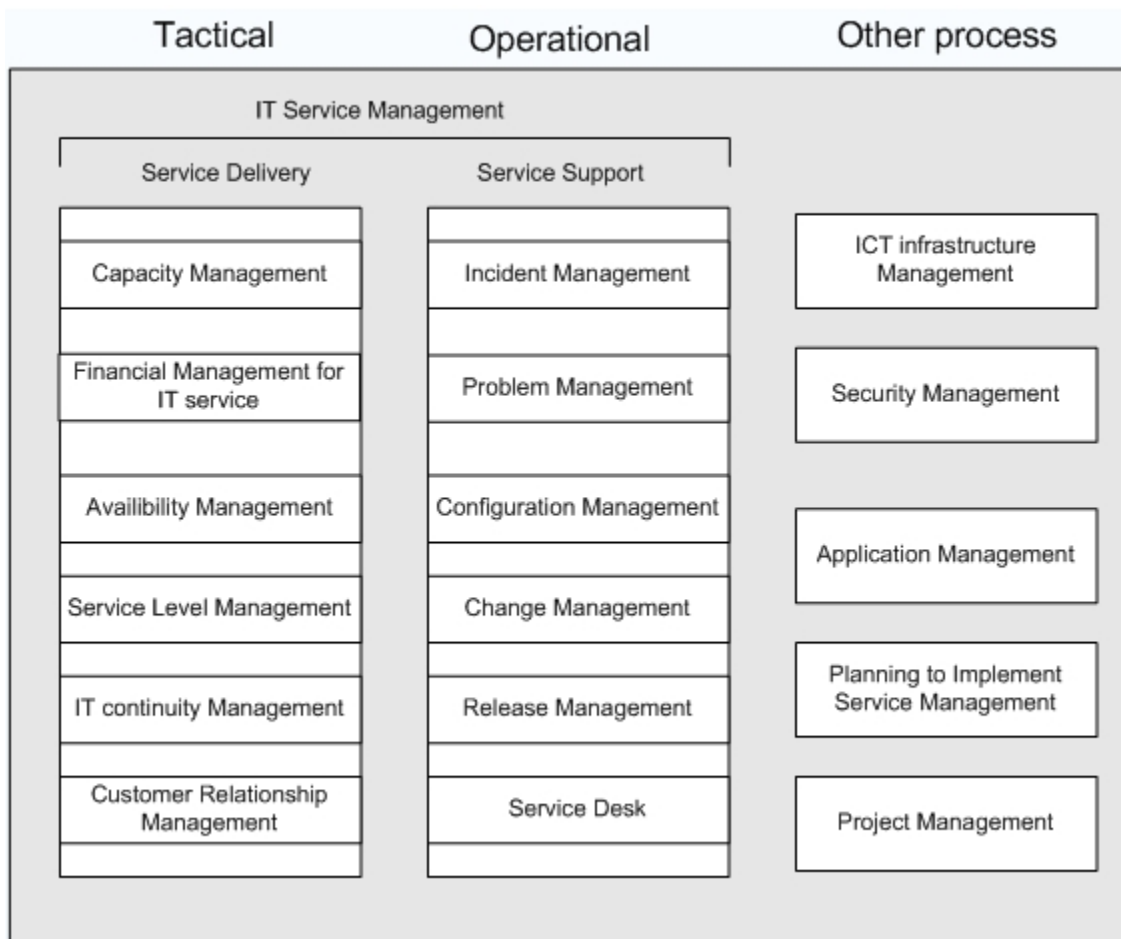
2007

WHAT IS ITIL

The ITIL (IT Infrastructure Library) consists of 5 volumes: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

Although the UK Government originally created the ITIL, it has rapidly been adopted across the world as the standard for best practice in the provision of information technology services.

As IT services become more closely aligned and integrated with the business, ITIL assists in establishing a business management approach and discipline to IT Service Management, stressing the complementary aspects of running IT like a business. Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services.



ITIL VERSION 2

Version 2 of ITIL (IT Infrastructure Library) consisted of 7 sets: Service Support; Service Delivery; Planning to Implement Service Management; ICT Infrastructure Management; Applications Management; Security Management; The Business Perspective. However, the main focus was generally divided into two main areas, known as ITIL Service Delivery and ITIL Service Support.

Service Delivery is the management of the IT services themselves, and involves a number of management practices to ensure that IT services are provided as agreed between the Service Provider and the Customer. It includes 5 disciplines: Service Level Management, Capacity Management, Continuity Management, Availability Management, and IT Financial Management

Service Support is the practice of those disciplines that enable IT Services to be provided effectively. The 6 Service Support disciplines are: Configuration Management, Incident Management, Problem Management, Change Management, Service/Help Desk and Release Management.



ITIL Service Delivery

Service Delivery is the management of the IT services themselves, and involves a number of management practices to ensure that IT services are provided as agreed between the Service Provider and the Customer.

Service Delivery consists of 5 disciplines. These are:

- Service Level Management
- Capacity Management
- Contingency Planning
- Availability Management
- IT Financial Management

Service Level Management

Service Level Management is the primary management of IT services, ensuring that agreed services are delivered when and where they are supposed to be delivered. The Service Level Manager is dependent upon all the other areas of Service Delivery providing the necessary support that ensures the agreed services are provided in a secure, efficient and cost effective manner.

There are a number of business processes that form part of Service Level Management. These are:

- Reviewing existing services
- Negotiating with the Customers
- Reviewing the underpinning contacts of 3rd party service providers
- Producing and monitoring the Service Level Agreement (SLA)
- Implementation of Service Improvement policy and processes
- Establishing priorities
- Planning for service growth
- Involvement in the Accounting process to cost services and recover these costs

Service Level Management and IT Security

IT Security is an integral part of Service Delivery, and as Service Level Management is the key discipline in providing Service Delivery, this process is also ultimately responsible for ensuring that IT Services are provided in a secure manner, and the availability of the services is maximized within cost and efficiency constraints. Contingency Planning also forms part of Service Delivery to ensure that services can be recovered/maintained in the event of a serious incident.

Capacity Management

Capacity Management is the discipline that ensures IT infrastructure is provided at the right time in the right volume at the right price, and ensuring that IT is used in the most efficient manner.

This involves input from many areas of the business to identify what services are (or will be) required, what IT infrastructure is required to support these services, what level of Contingency will be needed, and what the cost of this infrastructure will be.

These are inputs into the following Capacity Management processes:

- Performance monitoring
- Workload monitoring
- Application sizing
- Resource forecasting
- Demand forecasting
- Modeling

From these processes come the results of capacity management, these being the capacity plan itself, forecasts, tuning data and Service Level Management guidelines.

Continuity Management

Continuity Management / Disaster Recovery / Business Continuity

Continuity management is the process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures - reducing the risk of a disaster in the first instance.

Continuity management is so important that many organizations will not do business with IT service providers if contingency planning is not practiced within the service provider's organization. It is also a fact that many organizations that have been involved in a disaster where their contingency plan failed ceased trading within 18 months following the disaster.

Continuity management is regarded as the recovery of the IT infrastructure used to deliver IT Services, but many businesses these days practice the much further reaching process of Business Continuity Planning (BCP), to ensure that the whole end-to-end business process can continue should a serious incident occur.

Continuity management involves the following basic steps:

- Prioritizing the businesses to be recovered by conducting a Business Impact Analysis (BIA)
- Performing a Risk Assessment (aka Risk Analysis) for each of the IT Services to identify the assets, threats, vulnerabilities and countermeasures for each service.
- Evaluating the options for recovery
- Producing the Contingency Plan
- Testing, reviewing, and revising the plan on a regular basis

Availability Management

Availability Management is the practice of identifying levels of IT Service availability for use in Service Level Reviews with Customers.

All areas of a service must be measurable and defined within the Service Level Agreement (SLA).

To measure service availability the following areas are usually included in the SLA:

- Agreement statistics – such as what is included within the agreed service.
- Availability – agreed service times, response times, etc.
- Help Desk Calls – number of incidents raised, response times, resolution times.
- Contingency – agreed contingency details, location of documentation, contingency site, 3rd party involvement, etc.
- Capacity – performance timings for online transactions, report production, numbers of users, etc.
- Costing Details – charges for the service, and any penalties should service levels not be met.

Availability is usually calculated based on a model involving the Availability Ratio and techniques such as Fault Tree Analysis, and includes the following elements:

- Serviceability – where a service is provided by a 3rd party organization, this is the expected availability of a component.
- Reliability – the time for which a component can be expected to perform under specific conditions without failure.
- Recoverability – the time it should take to restore a component back to its operational state after a failure.
- Maintainability – the ease with which a component can be maintained, which can be both remedial or preventative.
- Resilience – the ability to withstand failure.
- Security – the ability of components to withstand breaches of security.

Availability Management and IT Security

IT Security is an integral part of Availability Management; this being the primary focus of ensuring IT infrastructure continues to be available for the provision of IT Services.

Some of the above elements are really the outcome of performing a risk analysis to identify any resilience measures to be put in place, identifying just how reliable elements are and how many problems have been caused as a result of system failure.

The risk analysis also recommends controls to improve availability of IT infrastructure such as development standards, testing, physical security, the right skills in the right place at the right time, etc.

IT Financial Management

IT Financial Management is the discipline of ensuring IT infrastructure is obtained at the most effective price (which does not necessarily mean cheapest), and calculating the cost of providing IT services so that an organization can understand the costs of its IT services. These costs may then be recovered from the Customer of the service.

Costs are divided into costing units:

- Equipment
- Software
- Organization (staff, overtime)
- Accommodation
- Transfer (costs of 3rd party service providers)

The costs are divided into Direct and Indirect costs, and can be Capital or Ongoing.

ITIL Service Support

Service Support is the practice of those disciplines that enable IT Services to be provided. Without these disciplines, it would be almost impossible to provide these IT Services, and at best in a very unmanaged and haphazard way.

The 6 Service Support disciplines are:

- Configuration Management
- Problem Management
- Incident Management
- Change Management
- Service / Help Desk
- Release Management

ITIL Configuration Management

Configuration Management is the implementation of a database (Configuration Management Database – CMDB) that contains details of the organization's elements that are used in the provision and management of its IT services. This is more than just an 'asset register', as it will contain information that relates to the maintenance, movement, and problems experienced with the Configuration Items.

The CMDB also holds a much wider range of information about items that the organization's IT Services are dependant upon. This range of information includes:

- Hardware
- Software
- Documentation
- Personnel

Configuration Management essentially consists of 4 tasks:

Identification – this is the specification, identification of all IT components and their inclusion in the CMDB.

Control – this is the management of each Configuration Item, specifying who is authorized to 'change' it.

Status – this task is the recording of the status of all Configuration Items in the CMDB, and the maintenance of this information.

Verification – this task involves reviews and audits to ensure the information contained in the CMDB is accurate.

Configuration Management and IT Security

Without the definition of all configuration items that are used to provide an organization's IT services, it can be very difficult to identify which items are used for which services. This could result in critical configuration items being stolen, moved or misplaced, affecting the availability of the services dependant upon them. It could also result in unauthorized items being used in the provision of IT services.

Incident & Problem Management

Incident/Problem Management is the resolution and prevention of incidents that affect the normal running of an organization's IT services. This includes ensuring that faults are corrected, preventing any recurrence of these faults, and the application of preventative maintenance to reduce the likelihood of these faults occurring in the first instance.

Incident/Problem Management and IT Security

The effective practice of both Incident and Problem Management will ensure that the availability of IT services is maximized, and could also protect the integrity and confidentiality of information by identifying the root cause of a problem.

ITIL Change Management

Change Management is the practice of ensuring all changes to Configuration Items are carried out in a planned and authorized manner. This includes ensuring that there is a business reason behind each change, identifying the specific Configuration Items and IT Services affected by the change, planning the change, testing the change, and having a back out plan should the change result in an unexpected state of the Configuration Item.

Change Management and IT Security

IT Security must be embedded into the change management process to ensure that all changes have been assessed for risks. This will include assessing the potential business impacts should the change produce undesired results.

If Change Management procedures are not effective, this may result in unauthorized changes to IT Services, which could have major impacts on the business, including financial loss, customer loss, market loss, litigation, and in the worse case scenario, even collapse of the business that the IT Services are there to support.

The ITIL Service Desk (Formerly the ITIL Help Desk)

Service/Help Desk

The Service/Help Desk plays an important part in the provision of IT Services. It is very often the first contact the business users have in their use of IT Services when something does not work as expected. The Service/Help Desk is a single point of contact for end users who need help. Without this, an organization could certainly face losses due to inefficiencies.

The two main focuses of the Service Desk are Incident Control and Communication.

There are different types of Help Desk, the selection of which is dependant upon what the business requires. Some Help Desks provide a simple call logging function, and escalate calls to more experienced and trained staff. Others provide a high degree of business and technical knowledge with the ability to solve most incidents at the time that the business user reports them.

Service/Help Desk Activities

Other than for the Call Centre, Service or Help Desks tend to embrace the following: receive all calls and e-mails on incidents; incident recording; incident prioritization, classification and escalation; search for a 'work around'; update the end user on progress; handle communication for other ITIL processes; report to management, process managers and customers on service desk performance.

Service Desk and IT Security

As the Service/Help Desk is generally the first contact a business user has when reporting something out of the ordinary, the skill and assiduity of the Help Desk staff can often prevent recurrence of incidents, and instigate measures that will limit the impact of any breaches in IT Security.

Release Management

This discipline of IT Service Management is the management of all software configuration items within the organization. It is responsible for the management of software development, installation and support of an organization's software products.

Software is often not regarded as a tangible asset because of its intangible nature, which results in it not being effectively controlled. There can be several versions of the same software within the organization, and there can also be unlicensed and illegal copies of externally provided software.

The practice of effective Software Control & Distribution involves the creation of a Definitive Software Library (DSL), into which the master copies of all software is stored and from here its control and release is managed. The DSL consists of a physical store and a logical store. The physical store is where the master copies of all software media are stored. This tends to be software that has been provided from an external source. The logical store is the index of all software and releases, versions, etc. highlighting where the physical media can be located. The logical store may also be used for the storage of software developed within the organization.

SC&D procedures include the management of the software Configuration Items and their distribution and implementation into a production environment. This will involve the definition of a release program suitable for the organization, the definition of how version control will be implemented, and the procedures surrounding how software will be built, released and audited.

Software Control & Distribution and IT Security

All three of the key areas of IT Security (Availability, Confidentiality, and Integrity) can be exposed as a direct result of inadequate software control and distribution. If software changes are badly managed and not fully tested, this can lead to problems if these changes reach the production environment by causing services to be unavailable. In addition, unauthorized software modifications can lead to fraud, viruses, and malicious damage to data files.

For these and other reasons, it is important that SC&D procedures are fully reviewed by a security assessment, to ensure that appropriate counter measures are in place to reduce the threats described above.

ITIL VERSION 3

The release of the new version of ITIL brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance.

It also brought a rationalization in the number of volumes included in the set, which now comprises the following:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

What's new in ITIL 3?

More focus on IT and business operating as an ecosystem (rather than IT isolated or just aligned with business)

The process-based model of ITIL is replaced with a lifecycle model that contains the processes needed to manage services within a lifecycle stage structure

New functions such as event management are to be built into the incident lifecycle

More emphasis on the Return on Investment of ITIL. This is to help raise awareness of ITIL and its benefits and gain the commitment of senior management

Enhanced with guidance on new IT strategies such as outsourcing

Designed to make it easier for ITIL to address specific vertical markets – core practices are supported by more detailed complementary content specific to industry, stakeholder and practice topics, making the library more practical

Will include guidance on compliance to governance such as Basel II and Sarbanes Oxley, other frameworks such as COBIT and methodologies such as Six Sigma. It will also add metrics (such as balanced scorecards)

Service Support and Service Delivery processes will be integrated into a service lifecycle

Request fulfillment separate from incident management to be a process on its own

ITIL Service Strategy

Service Strategy deals with the strategic management approach in respect of IT Service Management; strategic analysis, planning, positioning, and implementation relating to service models, strategies, and strategic objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.

The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL ® Service Lifecycle. Service Strategy decisions have far-reaching consequences including those related to delayed effect.

Topics include the development of markets, internal and external, service assets, service catalog, and implementation of strategy through the Service Lifecycle; setting objectives and expectations of performance towards serving customers and market spaces, and to identify, select, and prioritize opportunities. Assisting an organization to position itself to deal with the costs and risks associated with its service portfolios, establishing both operational effectiveness and distinctive performance.

ITIL Service Strategy Principles

The documented principles cover

- Value Creation
- Service Provider Types
- Service Assets
- Service Structures
- Service Strategy Fundamentals

ITIL Service Design

Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.

The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. Service Design is not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels. It also provides guidance on the development of design capabilities for service management.

ITIL Service Design Principles

The documented principles cover

- Business Change Process
- Balanced Design
- Design Constraints
- Design Activities
- Design Aspects
- Subsequent Design Activities
- Service Oriented Architecture
- Business Service management
- Service Design Models

ITIL Service Transition

Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.

The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations. Guidance is provided on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling the risks of failure and disruption. It combines the processes in Release, Program and Risk Management and sets them in the practical context of Service Management. Service Transition provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation. It provides guidance on transferring the control of services between customers and service providers.

ITIL Service Transition Principles

The documented principles cover

- Service Utilities
- Service Warranties

ITIL Service Operation

Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

This volume presents practices in the management of service operations and includes guidance on achieving efficiency and effectiveness in the delivery and support of services to ensure value for the customer and the service provider. Service operations ultimately fulfill the strategic objectives, which make it a critical capability. Guidance is provided on techniques to maintain service operations stability whilst allowing for changes in design, scope, scale, and service levels.

Service Operation provides detailed guidelines on processes, methods, and tools in addressing the proactive and reactive control perspectives. Managers and practitioners are provided with knowledge; enabling them to make better informed decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling of operations, and fixing problems.

ITIL Service Operation Principles

The documented principles cover

- Functions, Groups, Teams, Departments and Divisions
- Providing Service
- Achieving Balance in Service Operation
- Operation Staff involvement in Design/Transition
- Operational Health
- Documentation
- Communication

ITIL Continual Service Improvement

Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.

This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services. It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

It provides guidance on linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.

ITIL Continual Service Improvement Principles

The documented principles cover

- Continual Service Improvement and Organizational Change
- External and Internal Drivers
- Ownership
- SLM
- The Deming Cycle
- Knowledge Management
- Service management and improvement
- Benchmarks
- IT Governance
- Frameworks, Models, Standards and Quality Systems